AGILENT TECHNOLOGIES, INC.
Legal Department, DL429
Intellectual Property Administration
P. O. Box 7599
Loveland, Colorado 80537-0599

ATTORNEY DOCKET NO. 10003417-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Engel

Serial No.: 10/005,749 Examiner: Perungavoor, V.

Filing Date: November 7, 2001 Group Art Unit: 2132

Title: Secure Communication Protocol Utilizing a Private Key Delivered Via a Secure Protocol

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on .

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

□ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)(1)-(5)) for the total number of months checked below:

□	one month	$ 120.00
□	two months	$ 450.00
□	three months	$1020.00
□	four months	$1590.00

□ The extension fee has already been filled in this application.

☒ (b) Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 50-1078 the sum of $500.00 . At any time during the pendency of this application, please charge any fees required or credit any overpayment to Deposit Account 50-1078 pursuant to 37 CFR 1.25.

A duplicate copy of this transmittal letter is enclosed.

□ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date of Deposit:

OR

☒ I hereby certify that this paper is being facsimile transmitted to the Patent and Trademark Office on the date shown below.

Date of Facsimile: April 3, 2006

Typed Name: Calvin Ward

Signature:

Respectfully submitted,

Engel

By

Calvin B. Ward
Attorney/Agent for Applicant(s)

Reg. No. 30,896

Date: April 3, 2006

Telephone No. 925-855-0413

Rev 10/04 (ApBrief)

PATENT APPLICATION
Attorney Docket: 10003417-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS

Applicant:	Engel
Serial No.:	10/005,749
Filed:	11/7/2001
For:	Secure Communication Protocol Utilizing a Private Key Delivered via a Secure Protocol
Group Art Unit:	2132
Examiner:	Perungavoor, V.

BRIEF FOR APPELLANT

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the decision of the Primary Examiner dated 2/6/2006, finally rejecting Claims 1-8 in the above-identified patent application.

I. REAL PARTY IN INTEREST

The real party in interest is Agilent Technologies, Inc. having an address as shown below.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to appellant, the appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

III. STATUS OF THE CLAIMS

Claims 1-8 are currently pending in the above-identified patent application. In the Office Action dated 2/06/2006, the Examiner rejected Claims 1-8 and indicated that the Action was final.

IV. STATUS OF AMENDMENTS

No amendments have been filed since the final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Refer to Figure 1 and the discussion thereof that begins on page 3, at line 15 of the specification. The present invention is directed to computer networks in which a computer having limited computational resources (node 12) wishes to communicate with another computer (server 14) over an insecure network (network 17) using an encryption protocol that requires a key. The computationally limited computer receives the key with thc help of a third computer (workstation 21) having more computational capacity that utilizes a secure communication protocol to obtain the key from server 14.

With reference to Claim 1, the present invention is a method for operating a computer system having first, second, and third data processors connected by a network that includes network 13 and network 17, which is an insecure network. The first processor corresponds to node 12, and the second processor corresponds to server 14. The third processor is workstation 21. The second data processor (server 14) sends a key for a first encryption protocol to the third data processor (workstation 21) using a second encryption protocol. The third data processor (workstation 21) then forwards the key to the first data processor (node 12). The first data processor (node 12) then uses the key to send a message to the second data processor (server 14) using the key, the message being encrypted in the first encryption protocol. With reference to Claim 4, the process is initiated in response to a message from the first data processor to the second data processor.

With reference to Claim 2, node 12 has insufficient computational resources to execute the second encryption protocol used by server 14 to send the key to workstation 21. With reference to Claim 3, the second encryption protocol is a public key encryption protocol. With reference to Claim 5, network segment 17 is the internet. With reference to Claim 6,

network segment 13 includes a local area network. With reference to Claim 7, the local area network is more secure than network 17. With reference to Claim 8, the first encryption protocol requires less computational resources than the second encryption protocol.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Rejection of Claims 1-8 under 35 U.S.C. 102(b) as being anticipated by US Patent 4,458,109 to Mueller-Scholer ("Scholer").

VII. ARGUMENT

A. The Examiner's Burden under 35 U.S.C. 102

The Examiner has the burden of showing by reference to the cited art each claim limitation in the reference. Anticipation under 35 U.S.C. 102 requires that each element of the claim in issue be found either expressly or inherently in a single prior art reference. In re King, 231 USPQ 136, 138 (Fed. Cir. 1986); Kalman v. Kimberly-Clark Corp., 218 USPQ 781, 789 (Fed. Cir. 1983). The mere fact that a certain thing may result from a given set of circumstances is not sufficient to sustain a rejection for anticipation. *Ex parte Skinner*, 2 USPQ2d 1788, 1789 (BdPatApp&Int 1986). "When the PTO asserts that there is an explicit or implicit teaching or suggestion in the prior art, it must indicate where such a teaching or suggestion appears in the reference" (*In re* Rijckaert, 28 USPQ2d, 1955, 1957).

Under the doctrine of inherency, if an element is not expressly disclosed in a prior art reference, the reference will still be deemed to anticipate a subsequent claim if the missing element "is necessarily present in the thing described in the reference " Cont'l Can Co. v. Monsanto Co., 948 F.2d 1264, 1268, 20 USPQ2d 1746, 1749(Fed. Cir. 1991). "Inherent anticipation requires that the missing descriptive material is 'necessarily present,' not merely probably or possibly present, in the prior art." *Trintec Indus., Inc. v. Top-U.S.A. Corp.*, 295 F.3d 1292, 1295, 63 USPQ2d 1597, 1599 (Fed. Cir. 2002) (quoting *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999)).

B. Rejection of Claims 1, 3

Claim 1 deals with a communication protocol between three data processors on a network in which the second and third data processors are connected by an insecure network segment. Refer to Figure 1 of the present application. Two encryption protocols are used

during the communication. In the first step of the protocol, the second data processor (server 14) sends a message to the third data processor (workstation 21) containing an encryption key for a first encryption protocol. This message is sent using a second encryption protocol. The third data processor (workstation 21) then sends that key to the first data processor (node 12). The first data processor (node 12) then sends a message to the second data processor (server 14) using that key.

In the system taught in Schloer, a sender (A) sends a message to a receiver (B) and receives a receipt from a security station (SSS) that indicates that the receiver received the message in question. To determine if Schloer anticipates Claim 1, one must assign the three data processors in Schloer to the functions of the three data processors in Claim 1.

The Examiner stated that Scholer discloses the forwarding of keys using a security station service, where a second processor sends a key to a third processor as shown in the passage at col. 2, line 34-42. The passage in question refers to a communication from A to SSS in which A sends a key K using a protocol SK.A together with the message encoded with K to SSS. Hence, the Examiner is assigning the role of the second data processor in Claim 1 to terminal A and the role of the third data processor in Claim 1 to terminal SSS inSchloer. This leaves terminal B to fill the role of the first data processor of Claim 1.

To anticipate Claim 1, SSS would need to send the key, K, to terminal B and terminal B would need to send the message encrypted with K to terminal A, i.e., $<MSC>_K$ would need to go from B to A in Figure 1 of Schloer. This is clearly not the case.

Furthermore, no other assignment of the processors taught in Schloer will satisfy the limitations of Claim 1. Claim 1 requires that the second data processor sends the key to the third data processor, i.e., there is a message containing K that is sent from the second data processor. The only two data processors in Schloer that send the key in any form are terminal A, which sends it to SSS and SSS which sends it to both A and B in the RCPT message. As noted above, the assignment of A as the second processor results in a set of transmissions that do not satisfy the other limitations of Claim 1.

Consider the case in which SSS is the second data processor. Than one of A and B must be the third data processor and the other must be the first data processor. The claim requires that the third data processor forward the key to the first data processor. This limitation requires that there must be a message from A to B or from B to A containing the key, K. It should be noted that a message that is encrypted with the key is insufficient, since one cannot deduce the key from such a message. The only message between A and B taught in Schloer is the $<MSC>_K$ from A to B. This message does not contain the key K. Hence, Schloer could not anticipate Claim 1 or the claims dependent therefrom.

C. Rejection of Claim 2

In addition to the limitations of Claim 1, Claim 2 requires that the first data processor have insufficient computational resources to execute the second encryption protocol. Schloer teaches that the second protocol is the public key protocol, since it is that protocol that is used to send the key, K, in various messages. Hence, the first data processor would need to have insufficient computational resources to execute the public key encryption system. However, Schloer clearly teaches that all of the data processors communicate using the public key encryption system. Furthermore, as noted above, terminal SSS is not even a candidate for the first data processor.

The Examiner attempts to overcome these problems by stating that SSS lacks a keyboard and display, while the other terminals have these elements. Even if this reading of Schloer is correct, it does not imply that SSS lacks the computational resources in question. The Examiner has not pointed to any teaching in the art that a data processor without a keyboard and monitor cannot execute the public key encryption system. Accordingly, there are additional grounds for allowing Claim 2.

D. Rejection of Claim 4

In addition to the limitations of Claim 1, Claim 2 requires that the step of causing the second data processor to send an encryption key to the third data processor is initiated in response to a message from the first data processor to the second data processor. The Examiner maintains that the passage at column 5, lines 32-42 teaches that the key is sent in response to a message from the first processor to the second processor.

First, the passage cited by the Examiner refers to the existence of a third terminal, C, on the network, but is silent with respect to the limitations in question. Second, the protocol taught in Schloer is initiated in response to a message being sent from terminal A to both terminals SSS and terminal B. If SSS is assigned the role of the second terminal, then terminal A is the first terminal and terminal B is the third terminal. However, as noted above, this would require terminal B to send K to terminal A, which is clearly not the case.

The Examiner attempts to overcome these problems by stating that since all of the terminals share a network, each terminal receives all of the messages sent by the other terminals. First, the Examiner has not pointed to any teaching that messages between terminals A and SSS are received by terminal B or that messages between terminals B and SSS are received by terminal A. Second, the claim requires that the key be sent in response to a message from the first data processor to the second data processor. This requires that the data processor receives a message and acts on it. Accordingly, there are additional grounds for allowing Claim 4.

E. Rejection of Claim 5

In addition to the limitations of Claim 1, Claim 5 requires that the network segment connecting the second and third data processors comprises the internet. The Examiner points to col. 6, lines 56-66 of Schloer as teaching this limitation. The passage is question makes no mention of the internet. In fact, Applicant's attorney has searched the entire text version of Schloer for the term internet and did not find any reference to the internet. The Examiner attempts to overcome this problem by pointing to col. 13, lines 9-16 as anticipating the internet since Schloer discloses a public network key in this passage. Applicant must disagree. A public network key is a particular encoding scheme that is independent of the communication link on which the data is sent. This protocol is used to secure digital data on any insecure network including wireless telephone transmissions and local area networks. Since there are numerous other networks that could be used in the system taught inSchloer, the cited passage does not explicitly or implicitly anticipate the internet limitation. Hence, there are additional grounds for allowing Claim 5

F. Rejection of Claim 6

In addition to the limitations of Claim 1, Claim 6 requires that the network segment connecting the first and third data processors comprises a local area network. The Examiner points to the passage at col. 12, lines 15-24 as teaching this limitation. Once again, Applicant must disagree. Schloer refers to a communication network; however, is silent with respect to the form of that network. Since communication networks other than a local area network could equally function in the Schloer system, Schloer does not explicitly or implicitly teach the local area network limitation. Thus there are additional grounds for allowing Claim 6.

G. Rejection of Claim 7

In addition to the limitations of Claim 1, Claim 7 requires that the network segment connecting the first and third data processors has a higher level of security than the network segment connecting the second and third data processors. The Examiner points to the passage at col. 13, lines 47-61 as teaching this limitation. Once again, Applicant must disagree. The cited passage does not refer to the relative security of the network segments. The passage discusses various check sums and verification computations performed by terminal SSS. Furthermore, Applicant can find no mention of the relative security of the segments anywhere in Scholer. Hence, there are additional grounds for allowing Claim 7.

H. Rejection of Claim 8

In addition to the limitations of Claim 1, Claim 8 requires that the first encryption protocol requires less computational resources than the second encryption protocol. The Examiner points to the passages at col. 13, lines 33-46 and col. 5, lines 25-28 and Figure 2 as teaching this limitation. Once again, Applicant must disagree.

The first encryption protocol is the protocol used by first data processor to send a message to the second data processor. The second encryption protocol is the protocol used by the second data processor to send the encryption key to the third data processor. In the scheme taught inSchloer, the key, K, is sent in a message that is encoded in the public key system no matter which data processor sends it. Hence, the second encryption protocol used in the system taught in Schloer must be the public key system. The only other encryption scheme taught in Schloer for sending a message is the DES system based on K that is used to generate $<MSG>_K$. Hence, the first encryption protocol is the DES.

The passage referenced above refers to using the DES encryption system as the system for generating <MSG>$_K$. The Examiner maintains that it is commonly known that DES requires more computational resources than the public key system; however, the Examiner does not point to any place in the art where this "commonly known" fact can be found. However, for the sake of argument, assume that the Examiner is correct, that DES requires more computational resources than the public key system. The claim requires that the first encryption protocol, i.e. DES, requires less computational resources than the second encryption protocol, i.e., the public key system. But the Examiner states that it is commonly known that DES requires more computational resources than the public key system. Hence, the Examiner admits that Schloer does not teach the limitation in question. Accordingly, there are additional grounds for allowing Claim 8.

VII. CONCLUSION

Appellants respectfully submit that for the reasons of fact and law argued herein, the decision of the Examiner in finally rejecting Claims 1-8 should be reversed.

I hereby certify that this paper (along with any others attached hereto) is being sent via facsimile to fax number: 571-273-8300

Respectfully Submitted,

Calvin B. Ward
Registration No. 30,896
Date: April 3, 2006

Agilent Technologies, Inc.
Legal Department, M/S DL429
Intellectual Property Administration
P.O. Box 7599
Loveland, CO 80537-0599
Telephone (925) 855-0413
Telefax (925)855-9214

APPENDIX

THE CLAIMS ON APPEAL:

1. A method for operating a computer system having first, second, and third data processors connected by a network wherein said second and third data processors are connected by an insecure network segment, said method comprising the steps of:

causing said second data processor to send an encryption key for a first encryption protocol to said third data processor utilizing a second encryption protocol;

causing said third data processor to forward said encryption key to said first data processor; and

causing said first data processor to send a message to said second data processor utilizing said encryption key and said first encryption protocol, said message being sent over a communication path comprising said insecure network segment.

2. The method of Claim 1 wherein said first data processor has insufficient computational resources to execute said second encryption protocol.

3. The method of Claim 1 wherein said second encryption protocol is a public key encryption protocol.

4. The method of Claim 1 wherein said step of causing said second data processor to send an encryption key is initiated in response to a message from said first data processor to said second data processor.

5. The method of Claim 1 wherein said insecure network segment comprises the Internet.

6. The method of Claim 1 wherein said network segment connecting said first and third data processors comprises a local area network.

7. The method of Claim 1 wherein said first and third data processors are connected by a network segment that has a higher level of security than said insecure network segment.

8. The method of Claim 1 wherein said first encryption protocol requires less computational resources than said second encryption protocol

Evidence Appendix

none

Related Proceedings Appendix

none

PATENT APPLICATION
Attorney Docket: 10003417-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS

Applicant:	Engel
Serial No.:	10/005,749
Filed:	11/7/2001
For:	Secure Communication Protocol Utilizing a Private Key Delivered via a Secure Protocol
Group Art Unit:	2132
Examiner:	Perungavoor, V.

BRIEF FOR APPELLANT

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the decision of the Primary Examiner dated 2/6/2006, finally rejecting Claims 1-8 in the above-identified patent application.

I. REAL PARTY IN INTEREST

The real party in interest is Agilent Technologies, Inc. having an address as shown below.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to appellant, the appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

III. STATUS OF THE CLAIMS

Claims 1-8 are currently pending in the above-identified patent application. In the Office Action dated 2/06/2006, the Examiner rejected Claims 1-8 and indicated that the Action was final.

IV. STATUS OF AMENDMENTS

No amendments have been filed since the final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Refer to Figure 1 and the discussion thereof that begins on page 3, at line 15 of the specification. The present invention is directed to computer networks in which a computer having limited computational resources (node 12) wishes to communicate with another computer (server 14) over an insecure network (network 17) using an encryption protocol that requires a key. The computationally limited computer receives the key with the help of a third computer (workstation 21) having more computational capacity that utilizes a secure communication protocol to obtain the key from server 14.

With reference to Claim 1, the present invention is a method for operating a computer system having first, second, and third data processors connected by a network that includes network 13 and network 17, which is an insecure network. The first processor corresponds to node 12, and the second processor corresponds to server 14. The third processor is workstation 21. The second data processor (server 14) sends a key for a first encryption protocol to the third data processor (workstation 21) using a second encryption protocol. The third data processor (workstation 21) then forwards the key to the first data processor (node 12). The first data processor (node 12) then uses the key to send a message to the second data processor (server 14) using the key, the message being encrypted in the first encryption protocol. With reference to Claim 4, the process is initiated in response to a message from the first data processor to the second data processor.

With reference to Claim 2, node 12 has insufficient computational resources to execute the second encryption protocol used by server 14 to send the key to workstation 21. With reference to Claim 3, the second encryption protocol is a public key encryption protocol. With reference to Claim 5, network segment 17 is the internet. With reference to Claim 6,

network segment 13 includes a local area network. With reference to Claim 7, the local area network is more secure than network 17. With reference to Claim 8, the first encryption protocol requires less computational resources than the second encryption protocol.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Rejection of Claims 1-8 under 35 U.S.C. 102(b) as being anticipated by US Patent 4,458,109 to Mueller-Scholer ("Scholer").

VII. ARGUMENT

A. The Examiner's Burden under 35 U.S.C. 102

The Examiner has the burden of showing by reference to the cited art each claim limitation in the reference. Anticipation under 35 U.S.C. 102 requires that each element of the claim in issue be found either expressly or inherently in a single prior art reference. In re King, 231 USPQ 136, 138 (Fed. Cir. 1986); Kalman v. Kimberly-Clark Corp., 218 USPQ 781, 789 (Fed. Cir. 1983). The mere fact that a certain thing may result from a given set of circumstances is not sufficient to sustain a rejection for anticipation. *Ex parte Skinner*, 2 USPQ2d 1788, 1789 (BdPatApp&Int 1986). "When the PTO asserts that there is an explicit or implicit teaching or suggestion in the prior art, it must indicate where such a teaching or suggestion appears in the reference" (*In re* Rijckaert, 28 USPQ2d, 1955, 1957).

Under the doctrine of inherency, if an element is not expressly disclosed in a prior art reference, the reference will still be deemed to anticipate a subsequent claim if the missing element "is necessarily present in the thing described in the reference " Cont'l Can Co. v. Monsanto Co., 948 F.2d 1264, 1268, 20 USPQ2d 1746, 1749(Fed. Cir. 1991). "Inherent anticipation requires that the missing descriptive material is 'necessarily present,' not merely probably or possibly present, in the prior art." *Trintec Indus., Inc. v. Top-U.S.A. Corp.*, 295 F.3d 1292, 1295, 63 USPQ2d 1597, 1599 (Fed. Cir. 2002) (quoting *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999)).

B. Rejection of Claims 1, 3

Claim 1 deals with a communication protocol between three data processors on a network in which the second and third data processors are connected by an insecure network segment. Refer to Figure 1 of the present application. Two encryption protocols are used

during the communication. In the first step of the protocol, the second data processor (server 14) sends a message to the third data processor (workstation 21) containing an encryption key for a first encryption protocol. This message is sent using a second encryption protocol. The third data processor (workstation 21) then sends that key to the first data processor (node 12). The first data processor (node 12) then sends a message to the second data processor (server 14) using that key.

In the system taught in Schloer, a sender (A) sends a message to a receiver (B) and receives a receipt from a security station (SSS) that indicates that the receiver received the message in question. To determine if Schloer anticipates Claim 1, one must assign the three data processors in Schloer to the functions of the three data processors in Claim 1.

The Examiner stated that Scholer discloses the forwarding of keys using a security station service, where a second processor sends a key to a third processor as shown in the passage at col. 2, line 34-42. The passage in question refers to a communication from A to SSS in which A sends a key K using a protocol SK.A together with the message encoded with K to SSS. Hence, the Examiner is assigning the role of the second data processor in Claim 1 to terminal A and the role of the third data processor in Claim 1 to terminal SSS inSchloer. This leaves terminal B to fill the role of the first data processor of Claim 1.

To anticipate Claim 1, SSS would need to send the key, K, to terminal B and terminal B would need to send the message encrypted with K to terminal A, i.e., $<MSC>_K$ would need to go from B to A in Figure 1 of Schloer. This is clearly not the case.

Furthermore, no other assignment of the processors taught in Schloer will satisfy the limitations of Claim 1. Claim 1 requires that the second data processor sends the key to the third data processor, i.e., there is a message containing K that is sent from the second data processor.. The only two data processors in Schloer that send the key in any form are terminal A, which sends it to SSS and SSS which sends it to both A and B in the RCPT message. As noted above, the assignment of A as the second processor results in a set of transmissions that do not satisfy the other limitations of Claim 1.

Consider the case in which SSS is the second data processor. Than one of A and B must be the third data processor and the other must be the first data processor. The claim requires that the third data processor forward the key to the first data processor. This limitation requires that there must be a message from A to B or from B to A containing the key, K. It should be noted that a message that is encrypted with the key is insufficient, since one cannot deduce the key from such a message. The only message between A and B taught in Schloer is the $<MSC>_K$ from A to B. This message does not contain the key K. Hence, Schloer could not anticipate Claim 1 or the claims dependent therefrom.

C. Rejection of Claim 2

In addition to the limitations of Claim 1, Claim 2 requires that the first data processor have insufficient computational resources to execute the second encryption protocol. Schloer teaches that the second protocol is the public key protocol, since it is that protocol that is used to send the key, K, in various messages. Hence, the first data processor would need to have insufficient computational resources to execute the public key encryption system. However, Schloer clearly teaches that all of the data processors communicate using the public key encryption system. Furthermore, as noted above, terminal SSS is not even a candidate for the first data processor.

The Examiner attempts to overcome these problems by stating that SSS lacks a keyboard and display, while the other terminals have these elements. Even if this reading of Schloer is correct, it does not imply that SSS lacks the computational resources in question. The Examiner has not pointed to any teaching in the art that a data processor without a keyboard and monitor cannot execute the public key encryption system. Accordingly, there are additional grounds for allowing Claim 2.

D. Rejection of Claim 4

In addition to the limitations of Claim 1, Claim 2 requires that the step of causing the second data processor to send an encryption key to the third data processor is initiated in response to a message from the first data processor to the second data processor. The Examiner maintains that the passage at column 5, lines 32-42 teaches that the key is sent in response to a message from the first processor to the second processor.

First, the passage cited by the Examiner refers to the existence of a third terminal, C, on the network, but is silent with respect to the limitations in question. Second, the protocol taught in Schloer is initiated in response to a message being sent from terminal A to both terminals SSS and terminal B. If SSS is assigned the role of the second terminal, then terminal A is the first terminal and terminal B is the third terminal. However, as noted above, this would require terminal B to send K to terminal A, which is clearly not the case.

The Examiner attempts to overcome these problems by stating that since all of the terminals share a network, each terminal receives all of the messages sent by the other terminals. First, the Examiner has not pointed to any teaching that messages between terminals A and SSS are received by terminal B or that messages between terminals B and SSS are received by terminal A. Second, the claim requires that the key be sent in response to a message from the first data processor to the second data processor. This requires that the data processor receives a message and acts on it. Accordingly, there are additional grounds for allowing Claim 4.

E. Rejection of Claim 5

In addition to the limitations of Claim 1, Claim 5 requires that the network segment connecting the second and third data processors comprises the internet. The Examiner points to col. 6, lines 56-66 of Schloer as teaching this limitation. The passage is question makes no mention of the internet. In fact, Applicant's attorney has searched the entire text version of Schloer for the term internet and did not find any reference to the internet. The Examiner attempts to overcome this problem by pointing to col. 13, lines 9-16 as anticipating the internet since Schloer discloses a public network key in this passage. Applicant must disagree. A public network key is a particular encoding scheme that is independent of the communication link on which the data is sent. This protocol is used to secure digital data on any insecure network including wireless telephone transmissions and local area networks. Since there are numerous other networks that could be used in the system taught inSchloer, the cited passage does not explicitly or implicitly anticipate the internet limitation. Hence, there are additional grounds for allowing Claim 5

F. Rejection of Claim 6

In addition to the limitations of Claim 1, Claim 6 requires that the network segment connecting the first and third data processors comprises a local area network. The Examiner points to the passage at col. 12, lines 15-24 as teaching this limitation. Once again, Applicant must disagree. Schloer refers to a communication network; however, is silent with respect to the form of that network. Since communication networks other than a local area network could equally function in the Schloer system. Schloer does not explicitly or implicitly teach the local area network limitation. Thus there are additional grounds for allowing Claim 6.

G. Rejection of Claim 7

In addition to the limitations of Claim 1, Claim 7 requires that the network segment connecting the first and third data processors has a higher level of security than the network segment connecting the second and third data processors. The Examiner points to the passage at col. 13, lines 47-61 as teaching this limitation. Once again, Applicant must disagree. The cited passage does not refer to the relative security of the network segments. The passage discusses various check sums and verification computations performed by terminal SSS. Furthermore, Applicant can find no mention of the relative security of the segments anywhere in Scholer. Hence, there are additional grounds for allowing Claim 7.

H. Rejection of Claim 8

In addition to the limitations of Claim 1, Claim 8 requires that the first encryption protocol requires less computational resources than the second encryption protocol. The Examiner points to the passages at col. 13, lines 33-46 and col. 5, lines 25-28 and Figure 2 as teaching this limitation. Once again, Applicant must disagree.

The first encryption protocol is the protocol used by first data processor to send a message to the second data processor. The second encryption protocol is the protocol used by the second data processor to send the encryption key to the third data processor. In the scheme taught inSchloer, the key, K, is sent in a message that is encoded in the public key system no matter which data processor sends it. Hence, the second encryption protocol used in the system taught in Schloer must be the public key system. The only other encryption scheme taught in Schloer for sending a message is the DES system based on K that is used to generate $<MSG>_K$. Hence, the first encryption protocol is the DES.

The passage referenced above refers to using the DES encryption system as the system for generating <MSG>$_K$. The Examiner maintains that it is commonly known that DES requires more computational resources than the public key system; however, the Examiner does not point to any place in the art where this "commonly known" fact can be found. However, for the sake of argument, assume that the Examiner is correct, that DES requires more computational resources than the public key system. The claim requires that the first encryption protocol, i.e. DES, requires less computational resources than the second encryption protocol, i.e., the public key system. But the Examiner states that it is commonly known that DES requires more computational resources than the public key system. Hence, the Examiner admits that Schloer does not teach the limitation in question. Accordingly, there are additional grounds for allowing Claim 8.

VII. CONCLUSION

Appellants respectfully submit that for the reasons of fact and law argued herein, the decision of the Examiner in finally rejecting Claims 1-8 should be reversed.

I hereby certify that this paper (along with any others attached hereto) is being sent via facsimile to fax number: 571-273-8300

Respectfully Submitted,

Calvin B. Ward
Registration No. 30,896
Date: April 3, 2006

Agilent Technologies, Inc.
Legal Department, M/S DL429
Intellectual Property Administration
P.O. Box 7599
Loveland, CO 80537-0599
Telephone (925) 855-0413
Telefax (925)855-9214

APPENDIX

THE CLAIMS ON APPEAL:

1. A method for operating a computer system having first, second, and third data processors connected by a network wherein said second and third data processors are connected by an insecure network segment, said method comprising the steps of:

causing said second data processor to send an encryption key for a first encryption protocol to said third data processor utilizing a second encryption protocol;

causing said third data processor to forward said encryption key to said first data processor; and

causing said first data processor to send a message to said second data processor utilizing said encryption key and said first encryption protocol, said message being sent over a communication path comprising said insecure network segment.

2. The method of Claim 1 wherein said first data processor has insufficient computational resources to execute said second encryption protocol.

3. The method of Claim 1 wherein said second encryption protocol is a public key encryption protocol.

4. The method of Claim 1 wherein said step of causing said second data processor to send an encryption key is initiated in response to a message from said first data processor to said second data processor.

5. The method of Claim 1 wherein said insecure network segment comprises the Internet.

6. The method of Claim 1 wherein said network segment connecting said first and third data processors comprises a local area network.

7. The method of Claim 1 wherein said first and third data processors are connected by a network segment that has a higher level of security than said insecure network segment.

8. The method of Claim 1 wherein said first encryption protocol requires less computational resources than said second encryption protocol

Evidence Appendix

none

Related Proceedings Appendix

none

PATENT APPLICATION
Attorney Docket: 10003417-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS

Applicant:	Engel
Serial No.:	10/005,749
Filed:	11/7/2001
For:	Secure Communication Protocol Utilizing a Private Key Delivered via a Secure Protocol
Group Art Unit:	2132
Examiner:	Perungavoor, V.

BRIEF FOR APPELLANT

Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the decision of the Primary Examiner dated 2/6/2006, finally rejecting Claims 1-8 in the above-identified patent application.

I. REAL PARTY IN INTEREST

The real party in interest is Agilent Technologies, Inc. having an address as shown below.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to appellant, the appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

III. STATUS OF THE CLAIMS

Claims 1-8 are currently pending in the above-identified patent application. In the Office Action dated 2/06/2006, the Examiner rejected Claims 1-8 and indicated that the Action was final.

IV. STATUS OF AMENDMENTS

No amendments have been filed since the final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Refer to Figure 1 and the discussion thereof that begins on page 3, at line 15 of the specification. The present invention is directed to computer networks in which a computer having limited computational resources (node 12) wishes to communicate with another computer (server 14) over an insecure network (network 17) using an encryption protocol that requires a key. The computationally limited computer receives the key with the help of a third computer (workstation 21) having more computational capacity that utilizes a secure communication protocol to obtain the key from server 14.

With reference to Claim 1, the present invention is a method for operating a computer system having first, second, and third data processors connected by a network that includes network 13 and network 17, which is an insecure network. The first processor corresponds to node 12, and the second processor corresponds to server 14. The third processor is workstation 21. The second data processor (server 14) sends a key for a first encryption protocol to the third data processor (workstation 21) using a second encryption protocol. The third data processor (workstation 21) then forwards the key to the first data processor (node 12). The first data processor (node 12) then uses the key to send a message to the second data processor (server 14) using the key, the message being encrypted in the first encryption protocol. With reference to Claim 4, the process is initiated in response to a message from the first data processor to the second data processor.

With reference to Claim 2, node 12 has insufficient computational resources to execute the second encryption protocol used by server 14 to send the key to workstation 21. With reference to Claim 3, the second encryption protocol is a public key encryption protocol. With reference to Claim 5, network segment 17 is the internet. With reference to Claim 6,

network segment 13 includes a local area network. With reference to Claim 7, the local area network is more secure than network 17. With reference to Claim 8, the first encryption protocol requires less computational resources than the second encryption protocol.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Rejection of Claims 1-8 under 35 U.S.C. 102(b) as being anticipated by US Patent 4,458,109 to Mueller-Scholer ("Scholer").

VII. ARGUMENT

A. The Examiner's Burden under 35 U.S.C. 102

The Examiner has the burden of showing by reference to the cited art each claim limitation in the reference. Anticipation under 35 U.S.C. 102 requires that each element of the claim in issue be found either expressly or inherently in a single prior art reference. In re King, 231 USPQ 136, 138 (Fed. Cir. 1986); Kalman v. Kimberly-Clark Corp., 218 USPQ 781, 789 (Fed. Cir. 1983). The mere fact that a certain thing may result from a given set of circumstances is not sufficient to sustain a rejection for anticipation. *Ex parte Skinner*, 2 USPQ2d 1788, 1789 (BdPatApp&Int 1986). "When the PTO asserts that there is an explicit or implicit teaching or suggestion in the prior art, it must indicate where such a teaching or suggestion appears in the reference" (*In re* Rijckaert, 28 USPQ2d, 1955, 1957).

Under the doctrine of inherency, if an element is not expressly disclosed in a prior art reference, the reference will still be deemed to anticipate a subsequent claim if the missing element "is necessarily present in the thing described in the reference " Cont'l Can Co. v. Monsanto Co., 948 F.2d 1264, 1268, 20 USPQ2d 1746, 1749(Fed. Cir. 1991). "Inherent anticipation requires that the missing descriptive material is 'necessarily present,' not merely probably or possibly present, in the prior art." *Trintec Indus., Inc. v. Top-U.S.A. Corp.*, 295 F.3d 1292, 1295, 63 USPQ2d 1597, 1599 (Fed. Cir. 2002) (quoting *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999)).

B. Rejection of Claims 1, 3

Claim 1 deals with a communication protocol between three data processors on a network in which the second and third data processors are connected by an insecure network segment. Refer to Figure 1 of the present application. Two encryption protocols are used

during the communication. In the first step of the protocol, the second data processor (server 14) sends a message to the third data processor (workstation 21) containing an encryption key for a first encryption protocol. This message is sent using a second encryption protocol. The third data processor (workstation 21) then sends that key to the first data processor (node 12). The first data processor (node 12) then sends a message to the second data processor (server 14) using that key.

In the system taught in Schloer, a sender (A) sends a message to a receiver (B) and receives a receipt from a security station (SSS) that indicates that the receiver received the message in question. To determine if Schloer anticipates Claim 1, one must assign the three data processors in Schloer to the functions of the three data processors in Claim 1.

The Examiner stated that Scholer discloses the forwarding of keys using a security station service, where a second processor sends a key to a third processor as shown in the passage at col. 2, line 34-42. The passage in question refers to a communication from A to SSS in which A sends a key K using a protocol SK.A together with the message encoded with K to SSS. Hence, the Examiner is assigning the role of the second data processor in Claim 1 to terminal A and the role of the third data processor in Claim 1 to terminal SSS inSchloer. This leaves terminal B to fill the role of the first data processor of Claim 1.

To anticipate Claim 1, SSS would need to send the key, K, to terminal B and terminal B would need to send the message encrypted with K to terminal A, i.e., $<MSC>_K$ would need to go from B to A in Figure 1 of Schloer. This is clearly not the case.

Furthermore, no other assignment of the processors taught in Schloer will satisfy the limitations of Claim 1. Claim 1 requires that the second data processor sends the key to the third data processor, i.e., there is a message containing K that is sent from the second data processor. The only two data processors in Schloer that send the key in any form are terminal A, which sends it to SSS and SSS which sends it to both A and B in the RCPT message. As noted above, the assignment of A as the second processor results in a set of transmissions that do not satisfy the other limitations of Claim 1.

Consider the case in which SSS is the second data processor. Than one of A and B must be the third data processor and the other must be the first data processor. The claim requires that the third data processor forward the key to the first data processor. This limitation requires that there must be a message from A to B or from B to A containing the key, K. It should be noted that a message that is encrypted with the key is insufficient, since one cannot deduce the key from such a message. The only message between A and B taught in Schloer is the <MSC>$_K$ from A to B. This message does not contain the key K. Hence, Schloer could not anticipate Claim 1 or the claims dependent therefrom.

C. Rejection of Claim 2

In addition to the limitations of Claim 1, Claim 2 requires that thc first data processor have insufficient computational resources to execute the second encryption protocol. Schloer teaches that the second protocol is the public key protocol, since it is that protocol that is used to send the key, K, in various messages. Hence, the first data processor would need to have insufficient computational resources to execute the public key encryption system. However, Schloer clearly teaches that all of the data processors communicate using the public key encryption system. Furthermore, as noted above, terminal SSS is not even a candidate for the first data processor.

The Examiner attempts to overcome these problems by stating that SSS lacks a keyboard and display, while the other terminals have these elements. Even if this reading of Schloer is correct, it does not imply that SSS lacks the computational resources in question. The Examiner has not pointed to any teaching in the art that a data processor without a keyboard and monitor cannot execute the public key encryption system. Accordingly, there are additional grounds for allowing Claim 2.

D. Rejection of Claim 4

In addition to the limitations of Claim 1, Claim 2 requires that the step of causing the second data processor to send an encryption key to the third data processor is initiated in response to a message from the first data processor to the second data processor. The Examiner maintains that the passage at column 5, lines 32-42 teaches that the key is sent in response to a message from the first processor to the second processor.

First, the passage cited by the Examiner refers to the existence of a third terminal, C, on the network, but is silent with respect to the limitations in question. Second, the protocol taught in Schloer is initiated in response to a message being sent from terminal A to both terminals SSS and terminal B. If SSS is assigned the role of the second terminal, then terminal A is the first terminal and terminal B is the third terminal. However, as noted above, this would require terminal B to send K to terminal A, which is clearly not the case.

The Examiner attempts to overcome these problems by stating that since all of the terminals share a network, each terminal receives all of the messages sent by the other terminals. First, the Examiner has not pointed to any teaching that messages between terminals A and SSS are received by terminal B or that messages between terminals B and SSS are received by terminal A. Second, the claim requires that the key be sent in response to a message from the first data processor to the second data processor. This requires that the data processor receives a message and acts on it. Accordingly, there are additional grounds for allowing Claim 4.

E. Rejection of Claim 5

In addition to the limitations of Claim 1, Claim 5 requires that the network segment connecting the second and third data processors comprises the internet. The Examiner points to col. 6, lines 56-66 of Schloer as teaching this limitation. The passage is question makes no mention of the internet. In fact, Applicant's attorney has searched the entire text version of Schloer for the term internet and did not find any reference to the internet. The Examiner attempts to overcome this problem by pointing to col. 13, lines 9-16 as anticipating the internet since Schloer discloses a public network key in this passage. Applicant must disagree. A public network key is a particular encoding scheme that is independent of the communication link on which the data is sent. This protocol is used to secure digital data on any insecure network including wireless telephone transmissions and local area networks. Since there are numerous other networks that could be used in the system taught inSchloer, the cited passage does not explicitly or implicitly anticipate the internet limitation. Hence, there are additional grounds for allowing Claim 5

F. Rejection of Claim 6

In addition to the limitations of Claim 1, Claim 6 requires that the network segment connecting the first and third data processors comprises a local area network. The Examiner points to the passage at col. 12, lines 15-24 as teaching this limitation. Once again, Applicant must disagree. Schloer refers to a communication network; however, is silent with respect to the form of that network. Since communication networks other than a local area network could equally function in the Schloer system, Schloer does not explicitly or implicitly teach the local area network limitation. Thus there are additional grounds for allowing Claim 6.

G. Rejection of Claim 7

In addition to the limitations of Claim 1, Claim 7 requires that the network segment connecting the first and third data processors has a higher level of security than the network segment connecting the second and third data processors. The Examiner points to the passage at col. 13, lines 47-61 as teaching this limitation. Once again, Applicant must disagree. The cited passage does not refer to the relative security of the network segments. The passage discusses various check sums and verification computations performed by terminal SSS. Furthermore, Applicant can find no mention of the relative security of the segments anywhere in Scholer. Hence, there are additional grounds for allowing Claim 7.

H. Rejection of Claim 8

In addition to the limitations of Claim 1, Claim 8 requires that the first encryption protocol requires less computational resources than the second encryption protocol. The Examiner points to the passages at col. 13, lines 33-46 and col. 5, lines 25-28 and Figure 2 as teaching this limitation. Once again, Applicant must disagree.

The first encryption protocol is the protocol used by first data processor to send a message to the second data processor. The second encryption protocol is the protocol used by the second data processor to send the encryption key to the third data processor. In the scheme taught inSchloer, the key, K, is sent in a message that is encoded in the public key system no matter which data processor sends it. Hence, the second encryption protocol used in the system taught in Schloer must be the public key system. The only other encryption scheme taught in Schloer for sending a message is the DES system based on K that is used to generate $<MSG>_K$. Hence, the first encryption protocol is the DES.

The passage referenced above refers to using the DES encryption system as the system for generating <MSG>$_K$. The Examiner maintains that it is commonly known that DES requires more computational resources than the public key system; however, the Examiner does not point to any place in the art where this "commonly known" fact can be found. However, for the sake of argument, assume that the Examiner is correct, that DES requires more computational resources than the public key system. The claim requires that the first encryption protocol, i.e. DES, requires less computational resources than the second encryption protocol, i.e., the public key system. But the Examiner states that it is commonly known that DES requires more computational resources than the public key system. Hence, the Examiner admits that Schloer does not teach the limitation in question. Accordingly, there are additional grounds for allowing Claim 8.

VII. CONCLUSION

Appellants respectfully submit that for the reasons of fact and law argued herein, the decision of the Examiner in finally rejecting Claims 1-8 should be reversed.

I hereby certify that this paper (along with any others attached hereto) is being sent via facsimile to fax number: 571-273-8300

Respectfully Submitted,

Calvin B. Ward
Registration No. 30,896
Date: April 3, 2006

Agilent Technologies, Inc.
Legal Department, M/S DL429
Intellectual Property Administration
P.O. Box 7599
Loveland, CO 80537-0599
Telephone (925) 855-0413
Telefax (925)855-9214

APPENDIX

THE CLAIMS ON APPEAL:

1. A method for operating a computer system having first, second, and third data processors connected by a network wherein said second and third data processors are connected by an insecure network segment, said method comprising the steps of:

causing said second data processor to send an encryption key for a first encryption protocol to said third data processor utilizing a second encryption protocol;

causing said third data processor to forward said encryption key to said first data processor; and

causing said first data processor to send a message to said second data processor utilizing said encryption key and said first encryption protocol, said message being sent over a communication path comprising said insecure network segment.

2. The method of Claim 1 wherein said first data processor has insufficient computational resources to execute said second encryption protocol.

3. The method of Claim 1 wherein said second encryption protocol is a public key encryption protocol.

4. The method of Claim 1 wherein said step of causing said second data processor to send an encryption key is initiated in response to a message from said first data processor to said second data processor.

5. The method of Claim 1 wherein said insecure network segment comprises the Internet.

6. The method of Claim 1 wherein said network segment connecting said first and third data processors comprises a local area network.

7. The method of Claim 1 wherein said first and third data processors are connected by a network segment that has a higher level of security than said insecure network segment.

8. The method of Claim 1 wherein said first encryption protocol requires less computational resources than said second encryption protocol

Evidence Appendix

none

Related Proceedings Appendix

none